(12) UK Patent Application (19) GB (11) 2 381 173 (13) A

(43) Date of A Publication 23.04.2003

(21) Application No 0222978.9

(22) Date of Filing 04.10.2002

(30) Priority Data
(31) 0124681 (32) 15.10.2001 (33) GB

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto,
California 94304, United States of America

(72) Inventor(s)
Keith Alexander Harrison

(74) Agent and/or Address for Service
Chris Harrison
Hewlett-Packard Ltd IP Section,
Filton Road, Stoke Gifford, BRISTOL,
BS34 8QZ, United Kingdom

(51) INT CL[7]
H04L 9/30 29/06

(52) UK CL (Edition V)
H4P PDCSP

(56) Documents Cited
GB 2368755 A
EP 0354774 A2
WO 2001/011527 A2
JP 2001244924 A

(58) Field of Search
UK CL (Edition V) H4P
INT CL[7] H04L
Other: Online: WPI, EPODOC, PAJ, INSPEC

(54) Abstract Title
Method and apparatus for encrypting data

(57) A method for encrypting data 15 comprising deriving a public key using a first data set that defines an instruction or term of an agreement; encrypting a second data set with the derived public key to produce a third data set; providing the encrypted third data set to a recipient 16; providing the public key to a third party e.g. a trusted authority 17 such that on satisfaction of the instruction or term of an agreement the third party provides or releases an associated private key to the recipient to allow decryption of the encrypted second data set. Satisfaction of the term of an agreement could comprise reaching a specified date or of making a payment.

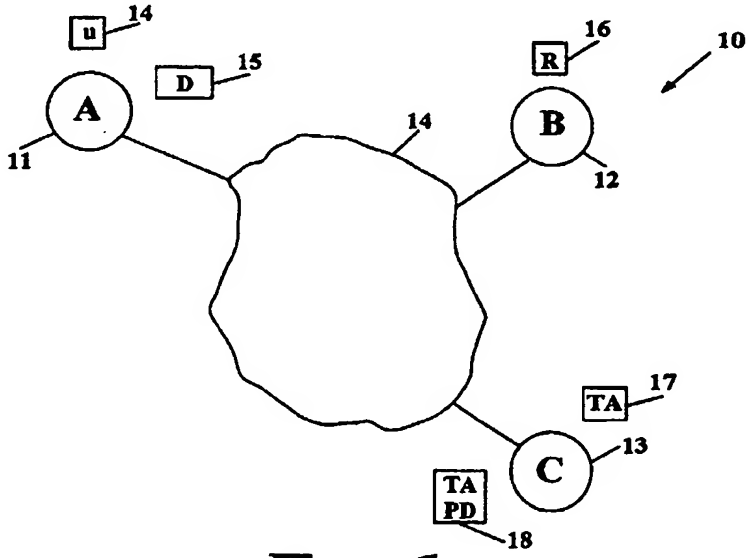

Fig. 1

GB 2 381 173 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

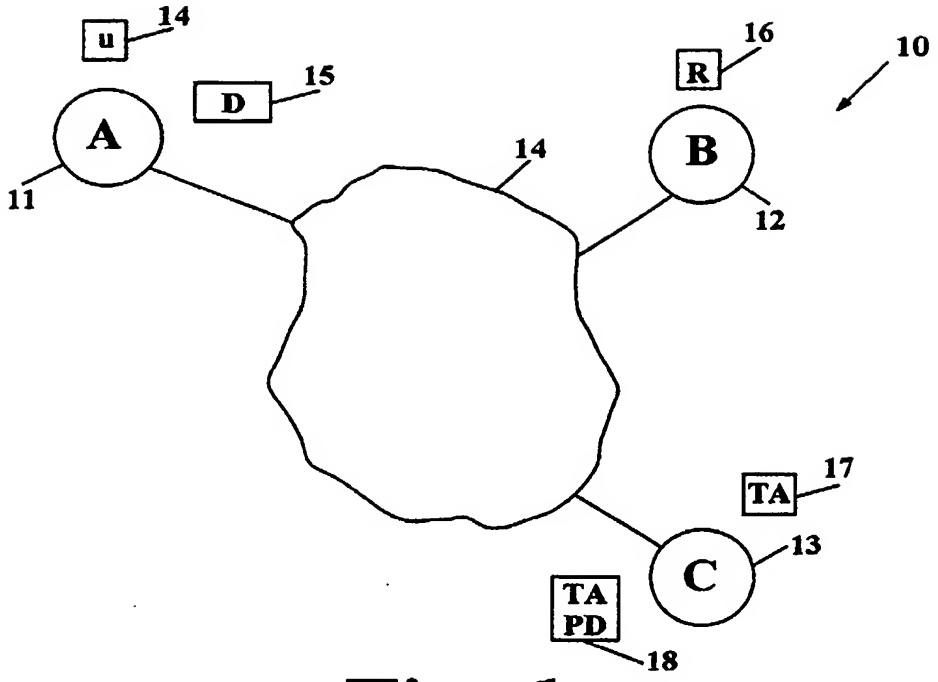

Fig. 1

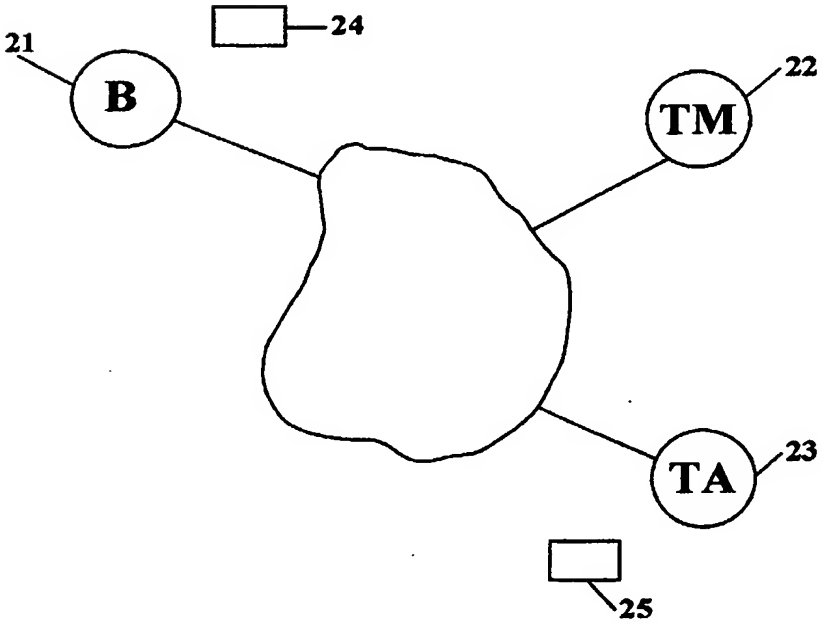

Fig 2

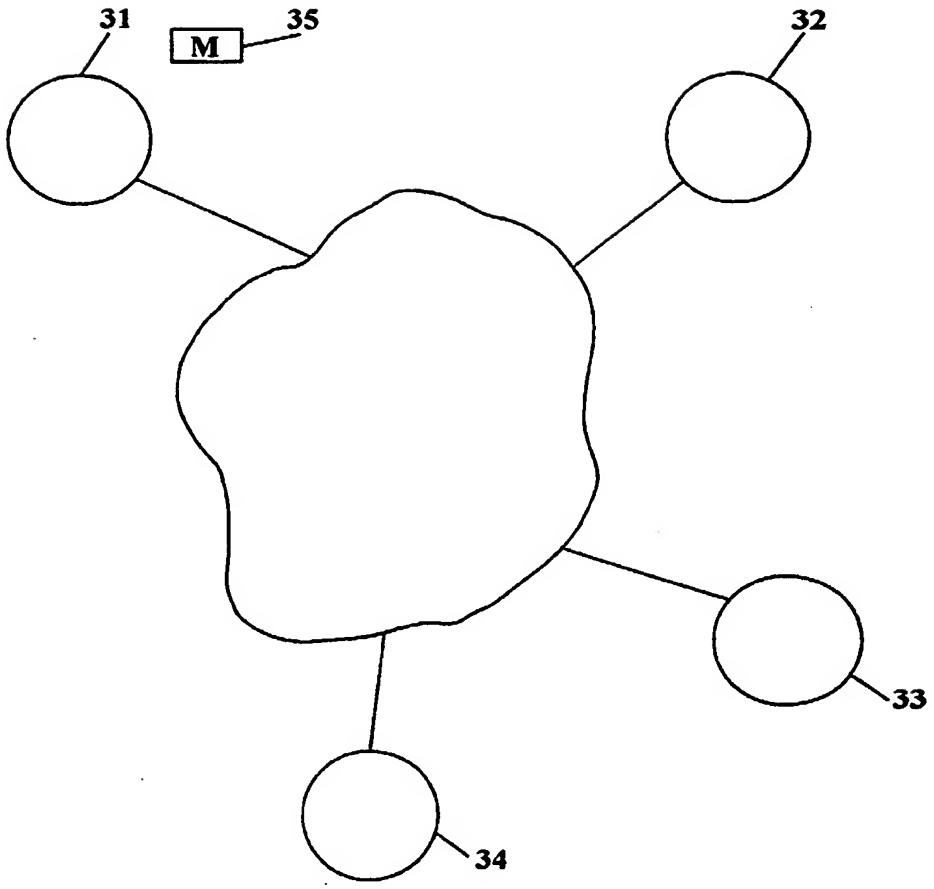

Fig 3

METHOD AND APPARATUS FOR ENCRYPTING DATA

The present invention relates to a method and system for encrypting data.

Escrow and PKI encryption are two techniques that have been utilised to allow information to be removed from the control of the information owner while still preventing other parties having access to the information until a predetermined condition has been met.

Two common examples where these techniques have been used are in sealed bids and music distribution. Seal bids require that all bids are submitted by a specified date where the originator of the bid needs to be satisfied that their bid is not disclosed before the specified date. Music distributors may wish to publish their music on a public database, where the music distributors needs to be satisfied that the intended user of the music can not listen to the music until they have paid for the use of the music. However, the setting up and use of escrow and PKI encryption can be complex.

It is desirable to improve this situation.

In accordance with a first aspect of the present invention there is provided a method for encrypting data comprising deriving a public key using a first data set that defines an instruction and a second data set associated with the third party; encrypting a third data set with the public key; providing the encrypted third data set to a recipient; providing the public key to the third party such that on satisfaction of the instruction the third party provides an associated private key to the recipient to allow decryption of the encrypted third data set.

In accordance with a second aspect of the present invention there is provided a method for encrypting data comprising deriving a public key using a first data set that defines a term of an agreement and a second data set associated with a third party; encrypting a third data set with the public key; providing the encrypted third data set to a recipient; providing the public key to the third party such that on satisfaction of the term of the agreement the third party provides an associated private key to the recipient to allow decryption of the encrypted third data set.

Preferably a term of the agreement that needs to be satisfied is that the private key should not be released to the recipient until a specified date.

Preferably a term of the agreement that needs to be satisfied to allow release of the private key to the recipient is the making of a payment.

Most preferably the encrypted third data set includes a nonce.

In accordance with a third aspect of the present invention there is provided a computer system for encrypting data comprising a first computer entity for deriving a public key using a first data set that defines a term of an agreement and a second data set associated with a third party and encrypting a third data set with the public key; communication means for providing the encrypted data to a second computer entity and the public key to a third computer entity; wherein the third computer entity is arranged, on satisfaction of the term of the agreement, to provide an associated private key to the second computer entity to allow decryption of the encrypted third data set.

In accordance with a forth aspect of the present invention there is provided a computer system for encrypting data comprising a first computer node for deriving a public key using a first data set that defines an instruction and a second data set associated with the third party and encrypting a third data set with the public key; communication means for providing the encrypted data to

a second computer node and the public key to a third computer node; wherein the third computer node is arranged, on satisfaction of the instruction to the third party, to provide an associated private key to the second computer node to allow decryption of the encrypted third data set.

In accordance with a fifth aspect of the present invention there is provided a computer apparatus for encrypting data comprising a processor for deriving a public key using a first data set that defines a term of an agreement and encrypting a second data set with the public key.

In accordance with a sixth aspect of the present invention there is provided a computer apparatus for encrypting data comprising a processor for deriving a public key using a first data set that defines an instruction and encrypting a second data set with the public key.

For a better understanding of the present invention and to understand how the same may be brought into effect reference will now be made, by way of example only, to the accompanying drawings, in which:-

Figure 1 illustrates a computer system according to an embodiment of the present invention;

Figure 2 illustrates a computer system arranged to support a sealed bid according to an embodiment of the present invention;

Figure 3 illustrates a computer system arranged to support a music distribution system according to an embodiment of the present invention.

The present invention addresses the issue of controlling access to data, where the owner/originator of the relevant data wishes to place conditions on the access to the data. This is achieved by using a public key to encrypt the

data where the public key itself stipulates the conditions under which access should be granted.

Figure 1 illustrates a computer system 10 according to an embodiment of the present invention. Computer system 10 includes a first computer entity 11, a second computer entity 12 and a third computer entity 13. Typically the three computer entities would be configured on separate computer platforms, however the computer entities 11, 12, 13 could be configured on a single computer platform. For the purposes of this embodiment, however, the three computer entities 11, 12, 13 are coupled via the internet 14.

Associated with the first computer entity 11 is a user 14 having data 15, for example a document, that they wish to make available, under certain conditions, to a third party. Associated with the second computer entity 12 is the intended recipient 16 of the data (i.e. the third party). Associated with the third computer entity 13 is a trust authority 17 (i.e. an authority that can be trusted by the user) for determining whether the conditions required for access to the data 15 and stipulated by the user 14 have been met. Additionally, the trust authority 17 makes publicly available the trust authorities public data 18, as described below. As would be appreciated by a person skilled in the art the trust authorities public data 18 can be made available in a variety of ways, for example via a web site.

Having selected the trust authority 17 as the appropriate trust authority for the intended purpose the user obtains the trust authorities public data 18; typically the user will have a selection of trust authorities from which to choose the one most appropriate.

The user 14 defines the terms and conditions for allowing access to the data. This string (i.e. the public encryption key), or typically a digital representation of this string, is then used to encrypt the user's data 15 (i.e. the data the user 14 wishes to control access too), as described below.

The user's terms and conditions can be expressed in any suitable language, for example XML where the following example illustrates the use of XML to encapsulate possible terms and conditions:

```
<termsAndConditions nonce="12345">
     <or>
          <dateAfter value="01/01/02">
          <and>
               <amount value="12.52UKP" account="xyz"/>
               <or>
                    <RequiredName name="NAME"/>
                    <RequiredRole name="Manager"/>
               </or>
          </and>
     </or>
</termsAndConditions>
```

The use of 'dataAfter' is used to instruct the trust authority not to release the associated private key to the recipient until after the '01/01/02'. Additionally, the terms and conditions require that an amount '12.52UKP' be paid by the recipient 16 before the trust authority releases the associated private key to the recipient 16.

The trust authorities public data 18 includes a hash function # and a value N that is a product of two random prime numbers p and q, where the values of p and q are only known to the trust authority 17.

The hash function # has the function of taking a string and returning a value in the range 0 to N-1. Additionally, the hash function # should have the jacobi characteristics: jacobi (#, N) = 1. That is to say, where $x^2 \equiv \# \bmod N$ the jacobi (#, N) = -1 if x does not exist, and = 1 if x does exist.

The values of p and q should ideally be in the range of 2^{511} and 2^{512} and should both satisfy the equation: $p,q \equiv 3 \bmod 4$. However, p and q must not have the same value.

To encrypt each bit M of the user's data 15 the user 14 generates random numbers t_+ (where t_+ is an integer in the range [0, 2^N)) until the user 14 finds a value of t_+ that satisfies the equation $jacobi(t_+, N) = M$, where M represents the individual binary digits 0, 1 of the user's data 15 as –1, 1 respectively. The user 14 then computes the value:

$$s_+ = (t_+ + \#(publickeystring)/t_+) \bmod N .$$

for each bit M where s_+ corresponds to the encrypted bit of M.

In case #(publickeystring) is non-square the user 14 additionally generates additional random numbers t_- (integers in the range [0, 2^N)) until the user 14 finds one that satisfies the equation $jacobi(t_-, N) = m$. The user 14 then computes the value:

$$s_- \equiv (t_- - \#(publickeystring)/t_-) \bmod N$$

for each value of bit M.

The encrypted data, together with the identity of the trust authority 17 and the public key, are made available to intended recipient 16 by any suitable means, for example via e-mail or by being placed in a electronic public area.

The public key, together with the identity of the intended recipient 16, is also made available to the trust authority 17 by any suitable means. Consequently,

the trust authority 17 is able to determine the terms and conditions that need to be satisfied to allow the trust authority 17 to issue the intended recipient 16 with the associated private key.

The trust authority 17 determines the associated private key B by solving the equation :

$$B^2 \equiv \#(publickeystring) \bmod N$$

If a value of B does not exist, then there is a value of B that is satisfied by the equation:

$$B^2 \equiv -\#(publickeystring) \bmod N$$

As N is a product of two prime numbers p, q it would be extremely difficult for any one to calculate the private key B with only knowledge of the public key string and N. However, as the trust authority 17 has knowledge of p and q (i.e. two prime numbers) it is relatively straightforward for the trust authority 17 to calculate B.

Any change to the public key will result in a private key that will not decrypt the document 15 correctly. Therefore, the intended recipient 16 cannot alter the public key before being supplied to the trust authority 17 and therefore cannot alter the relevant terms and conditions that apply to the release of the private key.

On receipt of the public key, the trust authority 17 checks whether the relevant terms and conditions have been met. When the trust authority 17 is satisfied that the terms and conditions have been met they supply the recipient 16 with the private key together with some indication of whether the public key is positive or negative.

If the square root of the encryption key returns a positive value, the users data M can be recovered using:

$$M = jacobi(s_+ + 2B, N).$$

If the square root of the encryption key returns a negative value, the users data M can be recovered using:

$$M = jacobi(s_- + 2B, N).$$

The recipient 16 then uses the appropriate equation above, in conjunction with the private key, to decrypt the message.

The recipient 16 may choose to cache the private key to decrypt the message 15 at a later date.

To prevent the reuse of the private key a nonce, i.e. a random number, can be incorporated into the terms and conditions. This ensures that the public key is unique thereby ensuring that the corresponding private key will also be unique.

Figure 2 illustrates the use of the present invention for the purposes of a seal bid arrangement, where bidder 21 provides authorization for the tender manager 22 to read the contents of the bidders seal bid 24 after a given data, for example once all bids have been received.

The bidder defines a set of terms and conditions using a suitable language, for example XML. The terms and conditions would include a date after which the bid details could be decrypted. For example:

```
<termsAndConditions nonce="1234">
     <and>
          <AccessorName name="NAME"/>
          <OpenAfter date="09:00 11/05/01"/>
     </and>
</termsAndConditions>
```

This string would be used as the public key to encrypt the document, in conjunction with the appropriate trust authorities 23 public details 25. The public key and the encrypted document would then be made available to the tender manager 22 by any suitable means.

In order for the tender manager 22 to obtain the respective private key the tender manager 22 sends the public key to the appropriate trust authority 23. The trust authority 23 would check that the requestor is the named tender manager and that the current date is after 09:00 11/05/01. Only when these conditions have been satisfied would the trust authority 23 release the private key, derived in accordance with the principles describe above. The nonce is included to ensure that the trust manager 23 will not have seen a public key identical to this in the past – and hence is not able to reuse an existing private key.

This embodiment only refers to a single trust authority, however, each bidder might choose a trust authority of their own choosing. The tender manager would then have to go to the appropriate trust authority to obtain the private key.

The language used to define the terms and conditions would be selected to allow expression of a variety of terms and conditions.

Figure 3 illustrates the use of the present invention for the purposes of enabling electronic distribution of music, where a music provider 31 provides

authorization for a recipient 32 to listen to the music after a specified payment has been made.

The prospective recipient 32 would retrieve the encrypted music, together with the public key used to encrypt the music 35 and the name of the appropriate trust authority 33. The encrypted music could be access, for example, via a public electronic database (not shown).

The public key might have the format:

```
<termsAndConditions nonce="1245">
     <Amount value="12.45UKP" account="xyz"/>
</termsAndConditions>
```

That is to say, the private key should only be release after the recipient 32 has paid a specified sum of money into a specified bank account 34.

In order for the music to be played it must be decrypted, which requires providing the public key to the appropriate trust authority 33, who can then determine what conditions have to be satisfied to allow release of the appropriate private key.

Any attempt on the part of the recipient to modify the terms and conditions would result in a public key that does not decrypt the music.

CLAIMS

1. A method for encrypting data comprising deriving a public key using a first data set that defines an instruction; encrypting a second data set with the public key; providing the encrypted third data set to a recipient; providing the public key to a third party such that on satisfaction of the instruction the third party provides an associated private key to the recipient to allow decryption of the encrypted second data set.

2. A method for encrypting data comprising deriving a public key using a first data set that defines a term of an agreement; encrypting a second data set with the public key; providing the encrypted second data set to a recipient; providing the public key to a third party such that on satisfaction of the term of the agreement the third party provides an associated private key to the recipient to allow decryption of the encrypted second data set.

3. A method according to claim 2, wherein a term of the agreement that needs to be satisfied is that the private key should not be released to the recipient until a specified date.

4. A method according to claim 2 or 3, wherein a term of the agreement that needs to be satisfied to allow release of the private key to the recipient is the making of a payment.

5. A method according to any preceding claim, wherein the second data set includes a nonce.

6. A method for encrypting data substantially as hereinbefore described with reference to the figures.

7. A computer system for encrypting data comprising a first computer entity for deriving a public key using a first data set that defines a term of an agreement and encrypting a second data set with the public key; communication means for providing the encrypted data to a second computer entity and the public key to a third computer entity; wherein the third computer entity is arranged, on satisfaction of the term of the agreement, to provide an associated private key to the second computer entity to allow decryption of the encrypted second data set.

8. A computer system for encrypting data comprising a first computer node for deriving a public key using a first data set that defines an instruction and encrypting a second data set with the public key; communication means for providing the encrypted data to a second computer node and the public key to a third computer node; wherein the third computer node is arranged, on satisfaction of the instruction to the third party, to provide an associated private key to the second computer node to allow decryption of the encrypted second data set.

9. A computer system for encrypting data substantially as hereinbefore described with reference to the figures.

10. A computer apparatus for encrypting data comprising a processor for deriving a public key using a first data set that defines a term of an agreement and encrypting a second data set with the public key.

11. A computer apparatus for encrypting data comprising a processor for deriving a public key using a first data set that defines an instruction and encrypting a second data set with the public key.

12. A computer apparatus for encrypting data substantially as hereinbefore described with reference to the figures.

INVESTOR IN PEOPLE

Application No: GB 0222978.9 **Examiner:** Adam Tucker
Claims searched: 1-12 **Date of search:** 30 January 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
A, P	-	GB 2368755 A	(Content Technologies) See in particular page 4 line 28-page 5 line 13
A	-	WO 01/11527 A2	(Yeda Research)
A	-	JP 2001244924	(Junya) See in particular supplied PAJ abstract and PAJ translated description and claims.
A	-	EP 0354774 A2	(IBM)

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

H4P

Worldwide search of patent documents classified in the following areas of the IPC[7]:

H04L

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, PAJ, INSPEC

INVESTOR IN PEOPLE

Application No: GB 0316027.2 **Examiner:** Joseph Wellings
Claims searched: 1-22 **Date of search:** 16 October 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
A, P		WO 02/077773 A2	(XANTE)
A		WO 98/16033 A1	(PROTOCALL)
A, P		GB 2381173 A	(HEWLETT-PACKARD)

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

H4P

Worldwide search of patent documents classified in the following areas of the IPC[7]:

G06F; H04L

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, PAJ